UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/473,522	12/28/1999	KENNETH A. PARULSKI	78744PRC	1080

1333 7590 02/06/2008
EASTMAN KODAK COMPANY
PATENT LEGAL STAFF
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER
GYORFI, THOMAS A

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
02/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

D

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/473,522
Filing Date: December 28, 1999
Appellant(s): PARULSKI ET AL.

Thomas J. Strouse
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed October 25, 2007 appealing from the Office action mailed July 25, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,889,324	KANAI	5-2005
6,046,768	KANEDA	4-2000

D. Eastlake et al. "RFC 1750: Randomness Recommendations for Security" December 1994, pages 1-30

Additionally, for purposes of illustrating inherent properties of the prior art, Examiner shall also refer to "Applied Cryptography, 2nd Edition" by Bruce Schneier, as was originally entered into the prosecution history in the Final Rejection of 7/12/05.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 2, and 4-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,889,324 (hereinafter, “Kanai”) in view of “RFC 1750: Randomness Recommendations for Security” (hereinafter, “Eastlake”).

Regarding claims 1, 6, 9, and 22:

Kanai discloses an improvement to various digital cameras comprising: a processor located within the digital camera for generating a random seed and generating a private key and a public key within the digital camera (col. 7, lines 34-51; col. 8, lines 1-7); and means for storing the private key in a memory of the digital camera for subsequent use of the hash of the digital image to produce the image authentication signature and the metadata signature (col. 4, lines 55-61).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera – in particular its inclusion of a CPU and RAM – are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer for the express purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 7:

Kanai discloses a method of authenticating an image captured by a digital camera, comprising: generating a random seed and generating a private key and a public key in the digital camera (col. 7, lines 34-51; col. 8, lines 1-7); storing the private key in a memory in the digital camera (col. 4, lines 55-61); communicating the public key to a user (Figure 5, step S204); capturing a digital image (col. 5, lines 10-15); hashing the captured digital image in the digital camera to produce an image hash (Figure 2, step S109; col. 6, lines 10-15); encrypting the image hash in the digital camera to produce a digital signature (Figure 2, step S110; col. 6, lines 15-20); and authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside the digital camera (col. 13, lines 1-11).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera – in particular its inclusion of a CPU and RAM – are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer for the express purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 8:

Kanai discloses a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising: manufacturing a digital camera with an internal processor for generating a random seed and generate a private key and a public key within the digital camera (col. 7, lines 34-51; col. 8, lines 1-7), storing the public key in a memory of the digital camera (col. 4, lines 55-61 and Figure 4), and communicating the public key to a camera operator (Figure 2, steps S204 and S206; col. 7, lines 43-49); sending the digital camera to an authentication service (the manufacturer: col. 7, lines 29-33); activating the digital camera at the authentication service to produce the private key and the public key, and registering the public key at the authentication service (col. 7, lines 29-51); and sending the digital camera to the user (implied by shipping out of the factory: col. 7, lines 29-33).

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section 5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera, and particularly its inclusion of a CPU and RAM, are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer specifically for the purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claim 10:

Kanai discloses a method of producing an image authentication signature in a digital camera, comprising: capturing a digital image (col. 5, lines 10-15); compressing the captured digital image (col. 5, lines 15-20); generating a random seed and generate a private key and a public key in the digital camera (col. 7, lines 34-51; col. 8, lines 1-7); storing the private key in a memory in the digital camera (col. 4, lines 55-61); providing one or more metadata values (Figure 2, step S108; col. 6, lines 7-12); hashing the compressed captured digital image and at least one of the metadata values to produce an image hash (Figure 2, step S109; col. 6, lines 10-15); and encrypting the image hash in the digital camera to produce an image authentication signature (Figure 2, step S110; col. 6, lines 15-20);

Kanai does not disclose the exact details of the key generating algorithms, particularly as they can be replaced (col. 8, lines 8-30). However, Eastlake teaches that algorithms to generate asymmetric key pairs, including those for digital signatures, typically require one or more random numbers (Eastlake, page 4, "Requirements", 4th paragraph) and furthermore states that one good source of random numbers can be generated entirely from the sensor noise of a digital camera (Eastlake, page 14, section

5.3.1, 1st paragraph; cf. pages 11-13 regarding the "easy" mathematical operations that a CPU such as in the Kanai camera could perform, required to de-skew the random number as part of the generating process). It would have been obvious to use sensor noise from the digital camera as the source for the random numbers in the key generation algorithm used by the CPU in the Kanai camera. The motivation for doing so would be to use a strong portable source of unpredictable numbers (Eastlake, Abstract, and page 10, section 5, "Hardware for Randomness").

Although the Eastlake reference may suggest that the computer and the camera are separate devices, it is noted that the internals of the Kanai camera, and particularly its inclusion of a CPU and RAM, are such that they could be regarded as a "computer" under the broadest reasonable interpretation of the term (see Kanai, Figure 1 and col. 4, line 35 – col. 5, line 10); furthermore, Examiner takes Official Notice that the ability of a camera to possess an onboard computer specifically for the purpose of generating cryptographic keys has long since been known in the art (pursuant to MPEP 2144.03, see U.S. Patent 5,801,856 to Moghadam et al., col. 4, lines 10-25, which discloses one such embodiment).

Regarding claims 2 and 23:

Kanai further discloses an image sensor for capturing images (Figure 1, element 20; col. 5, lines 5-15); and Eastlake discloses wherein the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the capture image is used in producing the random seed (page 14, section 5.3.1, 1st paragraph).

Regarding claim 4:

Kanai further discloses wherein the processor includes one or more algorithms for producing the random seed (col. 4, lines 45-51; col. 5, lines 30-35) wherein the random seed is used to produce a random number k (Ibid, and col. 8, lines 1-7), and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing (col. 10, lines 20-63).

Regarding claim 5:

Kanai further discloses wherein the processor includes an image processing algorithm using JPEG compression (col. 7, lines 10-12; col. 10, lines 15-20).

Regarding claim 11:

Kanai further discloses the step of storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values (Figure 9; and col. 9, line 44 – col. 10, line 12).

Regarding claim 12:

Kanai further discloses wherein the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature (col. 6, lines 10-20).

Regarding claim 13:

Kanai further discloses wherein the encrypting step includes encrypting the image hash with a private key to produce the image authentication signature (col. 6, lines 10-20), and further including the step of authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 13, lines 1-11; cf. col. 12, lines 24-67).

Regarding claim 14:

Kanai further discloses hashing the uncompressed capture digital image to produce a random number k (col. 6, lines 10-20), and wherein the encrypting step uses the random number k to produce the image authentication signature (Ibid).

Regarding claim 15:

Kanai further discloses wherein the encrypting step produces a metadata signature corresponding to the one or more metadata values (col. 12, lines 10-15).

Regarding claims 16-21:

Kanai further discloses the camera including firmware memory, wherein the private key is produced using an algorithm stored in firmware memory (col. 4, line 35 – col. 5, line 10). Kanai further discloses wherein the encryption and key generation algorithms can at least be updated, suggesting that it is not stored in immutable memory (col. 8, line 8 – col. 9, line 20); furthermore, in certain aspects/embodiments of the Kanai invention, the keys are generated once by the manufacturer prior to being shipped to an end user (col. 7, lines 29-33) and that the public should not be aware of the security algorithms used by the invention (col. 8, line 63 – col. 9, line 3 & lines 15-20). Taking all of these facts into account, it would have been obvious to one of ordinary skill in the art at the time the invention was made to delete the key generating algorithm from the memory of the Kanai camera once the manufacturer had generated the keys. The motivation for doing so would be that such an embodiment would require one less step – authenticating the cipher-processor is obviated – while still maintaining the overall security of the Kanai invention (Kanai: Figure 8, and col. 9, lines 1-8).

Regarding claim 24:

Eastlake further discloses wherein the random noise level is produced by random dark field image data taken from the sensor (as the image sensor is obstructed by another component of the camera: page 14, section 5.3.1, 1st paragraph)

Claims 3 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanai in view of Eastlake as applied to claims 2 and 24 above, and further in view of U.S. Patent 6,046,768 (hereinafter, "Kaneda").

Regarding claims 3 and 25:

Kanai further discloses an analog-to-digital converter coupled to the processor for producing digital signals corresponding to captured images (col. 5, lines 8-15); and

Eastlake discloses the processor causing the camera to be in a high gain condition when the initial test image is captured (page 14, section 5.3.1, 1st paragraph). However, neither reference explicitly discloses the use of a variable gain amplifier.

Kaneda discloses a variable gain amplifier coupled to an image sensor for use in a digital camera (Figure 34; col. 17, lines 37-50; col. 27, lines 1-10; col. 28, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate a variable gain amplifier into the camera disclosed by Kanai, resulting in the ability to amplify the gain as is required by Eastlake. One would be motivated to add a variable gain amplifier to a digital camera because they are also generally useful in correcting image blur from captured images (Kaneda, Ibid).

(10) Response to Argument

With respect to the rejection of claim 1, Appellant begins by arguing on page 6, line 12 – page 7, line 8 that the random number disclosed in Kanai (col. 8, lines 1-7) is not the same as the random seed used to generate a public key and a private key. Although Examiner concedes that Appellant's interpretation of this particular passage is correct, there is nevertheless sufficient evidence within the Kanai reference to establish that this limitation is inherent that invention. Specifically, as was pointed out in the previous Office Action, Kanai discloses wherein that camera possesses a key-generating algorithm by which the camera can create a public and private key pair (col. 7, lines 34-51). Kanai does not explicitly disclose the exact particulars of the key generating algorithm(s) that may be used, particularly as said algorithm can be updated or replaced as desired (col. 9, lines 9-20). Nevertheless, one of ordinary skill in the art would have known that regardless of the particular key generating algorithm, the first step is always to generate a random number. For illustration, the Schneier reference entered into the record on 7/12/05 clearly teaches that in order to generate keys for a public key cryptographic system (which is precisely the type of cryptography employed by Kanai: col. 4, lines 55-60), one must first generate random seeds that are just that: random (page 173, bottom paragraph). Schneier further discloses wherein all the known methods to generate the keys each begin by generating a random seed (pages 259-260, see step 1 for each of the Solovay-Strassen, Lehmann, and Rabin-Miller methods; cf. "Practical Considerations" on page 260). Thus the Kanai camera, in order to generate the keys via whichever key generating algorithm happens to be installed in a particular instance of that invention, must inherently have some facility to generate a random seed to perform the key generating process. The passage cited by the Examiner, and others such as col. 5, line 32, simply serves to illustrate that the Kanai camera does in fact have the ability to generate random numbers of its own accord. Since Kanai (a) needs a random number generator to generate keys, and (b) has a random number generator used for other functions in the same device, it would at the very least be obvious for Kanai (*prior* to any modification from Eastlake) to try using the random number generator as part of the key generating process, as a person of ordinary skill in the art would have good reason to pursue the known options within one's technical grasp. *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1395-96.

With regard to Appellant's argument on page 7, lines 9-17, Examiner fails to see how a teaching that the keys must be generated before any data measurement (which in the context of the Kanai reference is synonymous with taking a picture: col. 4, lines 15-35) somehow teaches away from the instant invention. To the contrary, at least one embodiment of the instant invention requires that the manufacturer, or a third party certification authority acting on behalf of the manufacturer, must activate the camera of the instant invention to generate the keys before the end-user is permitted to take any pictures (see the specification, page 8, lines 14-26). Similarly, Kanai discloses a similar arrangement (col. 7, lines 29-33). Furthermore, "data measurement" in the context of Kanai means that images generated by the camera are digitally signed to ensure their authenticity (col. 5, line 55 – col. 6, line 33). As disclosed in that passage, one must generate a key pair before any digital signatures can be made; similarly, in the instant invention, one must generate a key pair before one can employ the digital signature functionality of the device. There is no claim limitation or teaching in the specification that the random test image must itself be digitally signed, or "measured", prior to being used as a random seed.

With regard to Appellant's argument on page 7, line 18 – page 8, line 3, Examiner first wishes to note that whether or not the data measurement apparatus generates the keys in response to a signal from an external element is outside the scope of the claim. The claim only states, in general, that the various limitations regarding generating random seeds and private keys occur within the camera, but is silent regarding *how the camera is instructed to create the random seeds and keys in* *the first place*. The instant specification only teaches that this may occur when the camera is activated for the first time (page 6, lines 12-17), which neither teaches nor precludes the camera's key generation process from being activated by an external apparatus[1]; nor does the claim comprise language that states that the claimed method is initiated by, for example, a person pressing the power button of the camera for the first time. It is additionally observed that the involvement of the external apparatus in the key generation process is limited to receiving the public key after both the public and private keys have been generated by the digital measurement apparatus (col. 7, lines 34-43; cf. col. 3, lines 55-60, Figure 4, and elements S201-S204 of Figure 5) and to sign the public key creating a public-key certificate that is returned back to the digital measurement apparatus (col. 7, lines 43-51; elements S205-S027 of Figure 5). It is noted that the purpose of the public-key certificate in the Kanai invention is to establish that a certification authority attests that the public key contained therein is truly the public key belonging to the digital measurement apparatus (col. 2, line 62 – col. 3, line 5; col. 4, lines 55-60).

Second, it is observed that the involvement of the external device in the paragraph cited by the Appellant is limited to *updating* the key generation algorithm, not *executing* said key generating algorithm. Examiner could not find where in that passage Kanai would have disclosed wherein an external device generates the key; indeed, lines 15 -18 of column 9 only recite that the key generating algorithm is triggered by the

[1] It is also observed that the IC card, despite being referred to as an external device, is nevertheless a device physically inserted into the camera (col. 8, lines 5-15; cf. element 14 of Figure 2).

external authentication process, while Figure 4 actually discloses wherein the digital measurement apparatus (the camera, e.g. col. 4, lines 30-35) generates its keys internally with its algorithm (see also col. 7, lines 34-51). Moreover, even though Appellant alleges, "...Kanai may contemplate the authenticated external element supplying a random seed to the data measurement apparatus for use therein...",. Examiner formally requests Appellant to point to where Kanai discloses any such teaching. To the contrary, Kanai discloses that when the digital measurement apparatus needs to communicate with an IC card, it is the **digital measurement apparatus** that generates a random number and sends it to the IC card (col. 5, lines 30-35; col. 8, lines 1-7); the IC card, in response, returns the number in an encrypted fashion such that only the digital measurement apparatus should be able to decrypt it and verify that the encrypted random number matches the random number initially generated by the digital measurement apparatus (col. 5, lines 35-45; col. 8, Ibid). Additionally, the fact that Kanai teaches that the manufacturer may activate the key-generating process not only fails to teach away from the instant invention, but in actuality the instant application supports the same embodiment as was discussed in the previous paragraph(s) of this Answer: namely, that a certification authority may activate the camera to generate the key (page 8, lines 19-21), and that the certification authority may be the manufacturer itself (page 8, lines 16-18). Furthermore, Kanai was well aware of the security risks inherent in prior art cameras with digital signature capabilities, as known prior art devices required that the manufacturer would end up knowing the private key as a necessary consequence of generating the public and private key pair (col. 1, line 65 – col. 2, line 4); but by including key generating means internal to the camera, thus preventing the private key from ever being divulged to anyone, the manufacturer cannot know what the private key is (col. 2, lines 50-61) even though the manufacturer is the entity that activates the key generation algorithm (col. 7, lines 29-33). It is further observed that the instant invention recognizes this very same advantage regarding the manufacturer not being aware of the camera's private key (specification: page 1, lines 25-31; page 2, lines 25-30).

Continuing with Appellant's arguments on page 8, line 4 – page 9, line 16, Examiner disagrees with Appellant's overly narrow interpretation of the references. The Eastlake reference does not describe an invention *per se* but rather is a general discussion of techniques that were well known in the art by the time of the instant invention as to how one should generate good random numbers to be used for the very specific purpose of generating good keys for encryption algorithms (Eastlake, Abstract). In particular, one desirable method is to use thermal noise (page 10, "5. Hardware for Randomness", particularly the 2nd paragraph) and further that thermal noise can be generated *inter alia* by "a camera with the lens cap on" (page 14, section 5.3.1, 1st paragraph). It is additionally observed that, contrary to Appellant's argument, the word "external" never appears in the cited passages to discloses the combination of a computer and a camera. Obviously the digital measurement apparatus disclosed by Kanai comprises a camera; however, it is further observed that said digital measurement apparatus also comprises a CPU and RAM to execute various algorithms and store data (col. 4, line 36 – col. 5, line 10). Webster's II New Riverside University

Dictionary defines "computer" as "one that computes, esp. a high speed electronic device that processes, stores, and retrieves programmed information". In this vein, it is clear that at least the CPU component of the digital measurement apparatus comprises a "computer" under the broadest reasonable interpretation of the term, and therefore Kanai without any modification already discloses the configuration of a camera connected to a computer. Kanai, as has been established above, further requires some means to generate random numbers; and those of ordinary skill in the art have long since known that the best random numbers for key generation need to be truly random, as disclosed by Eastlake [as previously cited] and Schneier (e.g. page 173, last paragraph). Since the technique of using the image sensor of a camera to generate a random seed for key generation was clearly well known in the art, thus the combination of Kanai and Eastlake is nothing more than the predictable[2] use of prior art elements according to their established functions, which is sufficient to establish the obviousness of a claim over the prior art: *KSR,* 82 USPQ2d at 1396.

With respect to Appellant's argument on page 9, lines 17-26, Appellant attempts to argue that Eastlake further teaches away from the instant invention by arguing that additional computation is required after generating the thermal noise in order to produce the random seed, and that this somehow differs from the instant invention. This is incorrect, as this is precisely how the instant specification generates its random seed. To wit, Examiner quotes the instant specification, page 9, lines 9-19:

[2] In this case, the term "predictable" is understood to mean that the techniques disclosed by Eastlake are reliable for generating true random numbers, and **not** that the random sequences generated by the cited techniques are themselves predictable (like a pseudo-random generator: Eastlake, page 7, 1st para.)

> In a preferred approach depicted in FIG. 3, the random seed is generated by processing an image captured from the image sensor, which provides random dark field image data. In step 300, the variable gain amplifier 17 is set to provide a high level of gain. In step 310, an image is captured with the shutter 15 closed, and the raw CFA data from the image sensor 16 is temporarily stored in the RAM 24. The stored CFA data is composed of amplified dark current noise, so that each pixel value has a random noise level. **In step 320, the entire raw sensor image (or alternatively, a portion of the image) is then hashed down to 160 bits using the SHA-1 algorithm as specified in FIPS PUB 180-1.** The stored raw data is then deleted from the RAM 24 (step 330). **The 160 bit output of the SHA-1 is used as the random seed for the generation of x (step 340).**

(emphasis Examiner's)

As is plainly disclosed by the specification, and contrary to what Examiner believes is Appellant's argument, the raw image data generated by the camera of the instant invention is **not** used directly as the random seed, but is instead processed through an algorithm (the SHA-1 hashing algorithm) to produce a new value that is used as the random seed. Those of ordinary skill in the art would know that a hashing algorithm, such as SHA-1, requires exactly one input (in this case, the raw image data) and produces exactly one output (the random seed); thus, Examiner considered Appellant's claim limitation of "generating the random seed entirely from sensor noise of a digital camera" in this light: that additional processing can be used on the image data, provided that no other parameters are used in conjunction with the raw image data. Similarly, Eastlake discloses wherein random noise may need to be de-skewed (page 10, "5.2 Sensitivity to Skew") and proposes several methods to de-skew random noise (all of pages 11-13). As but one non-limiting example, Eastlake discloses that a compression algorithm may be used to de-skew the random noise thus making it suitable for use as a random seed (page 13, "5.2.4 Using Compression to De-skew"; cf. page 13, section 5.3.1, 3rd paragraph). Furthermore, the Kanai invention already comprises an image compression algorithm (JPEG[3]: col. 4, lines 48-50) wherein the compression algorithm receives one input (the raw image data) and produces one output (a compressed image, which according to Eastlake is a random seed: page 13, Ibid). Thus once again, it can be clearly seen that the combination of Eastlake with Kanai is merely a predictable combination of the known prior art elements according to their established functions.

With respect to Appellant's argument on page 9, line 27 - page 10, line 6, Appellant argues that fact that Kanai did not actually incorporate the teachings of Eastlake into that invention is somehow indicative of the claim being non-obvious, despite the Eastlake reference having long since been known in the art and predating all the other cited references. However, it is observed that the courts have held that the age of a reference does not preclude a finding of obviousness, absent a showing that the prior art tried and failed to solve the same problem notwithstanding its presumed knowledge of the references. See *In re Wright*, 569 F.2d 1124, 193 USPQ 332 (CCPA 1977). Appellant has shown no evidence that Kanai, or any other inventor, had attempted to incorporate the teachings of Eastlake into a digital camera and failed to achieve the combination. Furthermore, based on all the arguments above, Examiner maintains that the combination of references only takes into account knowledge which was within the level of ordinary skill of the art at the time the claimed invention was made, and does not include knowledge gleaned only from the Appellant's disclosure;

[3] See also the "JPEG (Transform Compression)" reference submitted in the Office Action of 7/25/07.

thus the combination of references is proper. *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Finally, with respect to the argument against Official Notice on page 10 of the Appeal Brief, it is observed that the cited passage discloses wherein the apparatus in question can be any one of (a) a camera with an attachable computer (col. 4, lines 12-15); (b) a camera with an onboard computer (col. 4, lines 15-16); or a separate light tight enclosure (Ibid). Appellant then points to Figure 2, which illustrates only embodiment (a) and erroneously concludes that this is the only embodiment where a computer stores the pertinent programs. However, the text is clear that the onboard computer is a substitute for the attachable computer, and in the context of the cited passage would perform the same function as the attachable computer. Nevertheless, in view of Examiner's above arguments regarding the use of a "computer" in the Kanai invention, and how the Kanai invention is capable of generating the key pair through a fully internalized process, Examiner believes this argument to be moot.

For at least all of the above reasons, Examiner respectfully submits that the rejection of claim 1 be upheld. As independent claims 9 and 10 are substantially similar to claim 1, thus Examiner respectfully submits that the rejections of claims 9 and 10 also be upheld. Examiner also respectfully submits that the rejections of dependent claims 4, 5, and 11-15 also be upheld for substantially similar reasons as above.

With respect to Appellant's argument for claim 2, Examiner fails to see how the references teach away from the instant invention. "Data measurement" in the context of Kanai means that images generated by the camera are digitally signed to ensure their authenticity (col. 5, line 55 – col. 6, line 33). As disclosed in that passage, one must generate a key pair before any digital signatures can be made; similarly, in the instant invention, one must generate a key pair before one can employ the digital signature functionality of the device. There is no claim limitation or teaching in the specification that the random test image must itself be digitally signed, or "measured", prior to being used as a random seed. Furthermore, Appellant's argument that the key generation algorithm being activated by an external authentication process somehow teaches away from the invention has already been discussed above; the key generation process is internal to the camera (col. 7, lines 34-51; col. 2, lines 50-61), and the claim has no limitation that would preclude an external trigger from activating the key generating algorithm. Finally, as has been discussed above, Eastlake teaches that the very purpose of using a camera with the lens cap on is to capture a random image so that its [thermal] noise level can be used to generate a random seed. It is further observed that just as Eastlake discusses obstructing the image sensor of the camera with another camera component (the lens cap), so too does the instant invention disclose that the image sensor works in conjunction with another component of the camera (the shutter) to generate a random noise image (specification: page 9, lines 12-13). So for at least all these reasons, Examiner respectfully submits that the rejection of claim 2 also be upheld. As Appellant's arguments for claims 6 and 7 are substantially similar to those above, Examiner thus respectfully submits that the rejections of claims 6 and 7 also be upheld for substantially similar reasons.

With respect to Appellant's arguments against the rejection of claim 8, it is observed that the instant specification teaches that "[t]he certification authority could be, for example, the camera manufacturer..." (specification, page 8, lines 16-17). Thus, in an embodiment where the claimed certification authority is the manufacturer, thus the limitation of sending the digital camera to the certification authority clearly becomes a trivial limitation; the claim does not limit the term "certification authority" to exclude the manufacturer itself. And as has been cited by both the Examiner and the Appellant, Kanai discloses wherein the manufacturer may be the entity that triggers the key generation process (col. 7, lines 29-33). The remaining arguments are substantially similar to those made by the Appellant regarding claim 1; thus for at least all of the above reasons, Examiner respectfully suggests that the rejection of claim 8 be upheld.

With respect to Appellant's arguments against the rejections of claim 16-21, it is observed that the only temporal constraint recited in the claim is that the algorithm is deleted "after the private key is generated"; however there is no requirement that the deletion must occur *immediately* after the private key is generated, nor that it occur within a preset time after the private key is generated. With that in mind, Kanai discloses that the algorithm to generate the key may be replaced (see col. 9, lines 8-21); this logically necessitates that the old algorithm is deleted and a new algorithm is installed in its place. So any instance of the Kanai invention where the algorithm to generate a new key pair is updated, no matter how much time has elapsed between the creation of the first private key and the update steps to create a second replacement private key, is sufficient for the Kanai reference to read on the claim. Thus Examiner respectfully submits that the rejections claims 16-21 be upheld for at least all of the above reasons.

Appellant's arguments with respect to claim 22 are substantially similar to those presented in response to the rejection of claim 1. Accordingly, Examiner respectfully submits that the rejection of claim 22 also be upheld for substantially similar reasons as discussed for claim 1 above.

Appellant's arguments with respect to claim 23 are substantially similar to those presented in response to the rejection of claim 2. Accordingly, Examiner respectfully submits that the rejection of claim 23 also be upheld for substantially similar reasons as discussed for claim 2 above.

With respect to Appellant's arguments regarding claim 24, once again Appellant has erroneously taken the teachings of Eastlake out of context. Eastlake recognized the need to perform some type of mathematical operation ("de-skewing": page 10, "5.2 Senstivity to Skew"; cf. page 13, section 5.3.1, "Combining this [thermal noise] with compression to de-skew..."). And has been already been discussed by the Examiner above, the instant invention does not trust the raw image noise to be used directly as a random seed, but itself performs a complex mathematical operation (the SHA-1 hashing algorithm, as per page 9, lines 15-20) and uses the output of said mathematical operation as the seed, *discarding the raw data* (Ibid). Thus Examiner fails to see any non-trivial[4] difference between the teachings of Eastlake and the instant invention that

[4] Please refer to Examiner's earlier comments on page 23 of this answer regarding the use of a component of a camera to obstruct the image sensor to create random/thermal noise.

would render the instant invention non-obvious over the prior art. So for at least all of the above reasons, Examiner respectfully submits that the rejection of claim 24 be upheld as well.

With respect to Appellant's argument for claim 3, Examiner fails to see how the references teach away from the instant invention. "Data measurement" in the context of Kanai means that images generated by the camera are digitally signed to ensure their authenticity (col. 5, line 55 – col. 6, line 33). As disclosed in that passage, one must generate a key pair before any digital signatures can be made; similarly, in the instant invention, one must generate a key pair before one can employ the digital signature functionality of the device. There is no claim limitation or teaching in the specification that the random test image must itself be digitally signed, or "measured", prior to being used as a random seed. Furthermore, Eastlake was already cited as illustrating the need for the thermal noise to be generated from a test image as requiring a high level of gain (page 13, "...a camera with the lens cap on, if the system has enough gain to detect anything, is essentially thermal noise"). Thus all that would be required to render the claim obvious is to find a showing that digital cameras could possess variable gain amplifiers; Kaneda, as cited in the Office Action discloses this. So at the very least where the claim is again merely the predictable use of prior art elements according to their known functions. *KSR*, 82 USPQ2d at 1396. It is also noted that the fact that Appellant has recognized another advantage from the use of variable gain amplifiers which would flow naturally from following the suggestion of the prior art (and specifically, the Eastlake reference) cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). So for at least all of the above reasons, Examiner respectfully submits that the rejection of claim 3 be upheld as well.

Appellant's arguments with respect to claim 25 are substantially similar to those presented in response to the rejection of claim 3. Accordingly, Examiner respectfully submits that the rejection of claim 25 also be upheld for substantially similar reasons as discussed for claim 2 above.

For all of the above reasons, the Examiner respectfully request that the Board of Patent Appeals and Interferences uphold the rejections of claims 1-25.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thomas Gyorfi

Examiner, Art Unit 2135

Conferees:

Kim Vu

Supverisory Examiner, AU2135

HOSUK SONG
PRIMARY EXAMINER

Hosuk Song HS

Primary Examiner, Art Unit 2135